

# COUNTING DEGENERATE POLYNOMIALS OF FIXED DEGREE AND BOUNDED HEIGHT

ARTŪRAS DUBICKAS AND MIN SHA

**ABSTRACT.** In this paper, we give sharp upper and lower bounds for the number of degenerate monic (and arbitrary, not necessarily monic) polynomials with integer coefficients of fixed degree  $n \geq 2$  and height bounded by  $H \geq 2$ . The polynomial is called *degenerate* if it has two distinct roots whose quotient is a root of unity. In particular, our bounds imply that non-degenerate linear recurrence sequences can be generated randomly.

## 1. INTRODUCTION

Recall that every linear recurrence sequence  $s_0, s_1, s_2, \dots$  of order  $n \geq 2$  satisfies the linear relation

$$(1.1) \quad s_{k+n} = a_1 s_{k+n-1} + \dots + a_n s_k \quad (k = 0, 1, 2, \dots).$$

Here, we suppose that the coefficients  $a_1, \dots, a_n$  and the initial values  $s_0, \dots, s_{n-1}$  of the sequence are some elements of a number field  $K$ , where  $a_n \neq 0$  and  $s_j \neq 0$  for at least one  $j$  in the range  $0 \leq j \leq n-1$ . The characteristic polynomial of this linear recurrence sequence is

$$f(X) = X^n - a_1 X^{n-1} - \dots - a_n \in K[X].$$

The sequence (1.1) is called *degenerate* if  $f$  has a pair of distinct roots whose quotient is a root of unity; otherwise the sequence (1.1) is called *non-degenerate*. It is well-known that the sequence (1.1) may have infinitely many zero terms only if it is degenerate, whereas the non-degenerate sequences contain only finitely many zero terms. See, for instance, [13, Section 2.1] for more details and more references.

Since non-degenerate linear recurrence sequences have much more applications in practice, it is important to investigate how often they occur. If we choose  $a_1, \dots, a_n$  as rational integers (or rational numbers), the results of this paper imply that almost every linear recurrence sequence generated randomly is non-degenerate.

---

2010 *Mathematics Subject Classification.* Primary 11C08; Secondary 11B37, 11R06.

*Key words and phrases.* Degenerate polynomial, linear recurrence sequence, Mahler measure, resultant.

By adopting this terminology, we say that a polynomial  $f \in \mathbb{C}[X]$  is *degenerate* if it has a pair of distinct roots whose quotient is a root of unity. Note that there already exist some methods for testing whether a given polynomial with integer coefficients is degenerate or not, see, e.g., [7]. In the sequel, all the polynomials we consider have integer coefficients except in few cases when this will be indicated explicitly.

We first define the set  $S_n(H)$  of degenerate monic polynomials with integer coefficients of degree  $n \geq 2$  and of height at most  $H$ , that is,

$$S_n(H) = \{f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X] : \\ f \text{ is degenerate, } |a_j| \leq H, j = 1, \dots, n\}.$$

Throughout, the height of a polynomial is defined to be the largest modulus of its coefficients. Then, we define

$$D_n(H) = |S_n(H)|,$$

where  $|A|$  is the cardinality of the set  $A$ .

To state our results we shall use the following standard notation. Throughout the paper, we use the Landau symbol  $O$  and the Vinogradov symbol  $\ll$ . Recall that the assertions  $U = O(V)$  and  $U \ll V$  (sometimes we will write this also as  $V \gg U$ ) are both equivalent to the inequality  $|U| \leq CV$  with some constant  $C > 0$ . In this paper, the constants implied in the symbols  $O, \ll$  and in the phrase “up to some constant” only depend on the degree  $n$ ; also, when we say “finitely many”, this means that the exact quantity also depends on the degree  $n$  only. In the sequel, we always assume that  $H$  is a positive integer (greater than 1 if there is the factor  $\log H$  in the corresponding formula), and  $n$  is an integer greater than 1.

The main result of this paper is the following:

**Theorem 1.1.** *For any integers  $n \geq 2$  and  $H \geq 2$ , we have the following sharp bounds for  $D_n(H)$ :*

$$\begin{aligned} H &\ll D_2(H) \ll H, \\ H \log H &\ll D_3(H) \ll H \log H, \\ H^{n-2} &\ll D_n(H) \ll H^{n-2} \quad (n \geq 4). \end{aligned}$$

When  $n$  is fixed, Theorem 1.1 says that the proportion of degenerate monic polynomials among the monic polynomials of degree  $n$  and height at most  $H$  tends to zero as  $H \rightarrow \infty$ . So, degenerate polynomials cannot be efficiently constructed by a random generation. It is easy to construct reducible degenerate polynomials. But it is not easy to construct irreducible degenerate polynomials of high degree  $n$  other than polynomials of the form  $g(X^\ell)$  or  $\prod_{j=1}^\ell g(\xi_j X)$  with irreducible (and

satisfying some further restrictions)  $g \in \mathbb{Z}[X]$  of degree  $n/\ell$ , where  $\xi_1, \dots, \xi_\ell$  are the conjugates of a root of unity  $\xi_1$  of degree  $\ell$ . Several other examples can be found in [7].

In order to obtain lower and upper bounds on the number  $D_n(H)$ , we define  $I_n(H)$  and  $R_n(H)$  as the numbers of irreducible and reducible polynomials  $f \in S_n(H)$ , respectively, so that

$$D_n(H) = I_n(H) + R_n(H).$$

In fact, by an explicit construction, it is quite easy to obtain the claimed lower bound for  $D_n(H)$ , whereas all the difficulties lie in getting the claimed upper bound for  $D_n(H)$ . Our approach is to first estimate  $I_n(H)$  and  $R_n(H)$ , respectively, and then sum them up.

Now, we state the following sharp estimates for  $I_n(H)$  and  $R_n(H)$ , and, furthermore, we discover an interesting phenomenon.

**Theorem 1.2.** *Let  $n \geq 2$  and  $H \geq 1$  be two integers, and let  $p$  be the smallest prime divisor of  $n$ . Then*

$$H^{n/p} \ll I_n(H) \ll H^{n/p}.$$

For  $R_n(H)$ , our bounds are the following:

**Theorem 1.3.** *For integers  $n \geq 2$  and  $H \geq 2$ , we have*

$$R_2(H) = \lfloor \sqrt{H} \rfloor,$$

$$H \log H \ll R_3(H) \ll H \log H,$$

$$H^{n-2} \ll R_n(H) \ll H^{n-2} \quad (n \geq 4).$$

From Theorems 1.2 and 1.3, for each  $n \geq 5$ , we have  $HI_n(H) \ll R_n(H)$ . Roughly speaking, most of the degenerate monic polynomials of degree  $n \geq 5$  are reducible. The reason why this is of interest is that the proportion of reducible monic polynomials of degree  $n \geq 2$  among all the monic polynomials of degree  $n$  and height at most  $H$  tends to zero as  $H \rightarrow \infty$ . However, in the set  $S_n(H)$ ,  $n \geq 5$ , the proportion of irreducible polynomials tends to zero as  $H \rightarrow \infty$ .

It is easy to see that Theorem 1.1 is a direct corollary of Theorems 1.2 and 1.3. We will prove Theorems 1.2 and 1.3 in Sections 3 and 4, respectively.

Actually, in a similar way we can count the number of degenerate (not necessarily monic) polynomials with integer coefficients of fixed degree and bounded height. Consider the set

$$S_n^*(H) = \{f(X) = a_0X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X] : \\ a_0 \neq 0, f \text{ is degenerate}, |a_j| \leq H, j = 0, 1, \dots, n\}.$$

Put  $D_n^*(H) = |S_n^*(H)|$ . As above, define  $I_n^*(H)$  and  $R_n^*(H)$  as the numbers of irreducible and reducible polynomials  $f \in S_n^*(H)$ , respectively, so that

$$D_n^*(H) = I_n^*(H) + R_n^*(H).$$

To make these definitions precise, we recall that, in general, a non-zero non-unit element of a commutative ring  $R$  is said to be *irreducible* if it is not a product of two non-units and *reducible* otherwise. In this paper, the polynomials in  $\mathbb{Z}[x]$  are called irreducible if they are irreducible in the ring  $\mathbb{Q}[x]$ . Note that there is a slight difference between the irreducibility of a polynomial with integer coefficients in the rings  $\mathbb{Z}[x]$  and  $\mathbb{Q}[x]$ . For example, any linear polynomial is irreducible in  $\mathbb{Q}[x]$ , but, e.g.,  $ax + a$  with integer  $a \geq 2$ , is reducible in  $\mathbb{Z}[x]$ , whereas the polynomial  $x^2 - 1$  is reducible in both rings  $\mathbb{Z}[x]$  and  $\mathbb{Q}[x]$ .

The analogue of Theorem 1.1 can be stated as follows:

**Theorem 1.4.** *For any integers  $n \geq 2$  and  $H \geq 2$ , we have*

$$\begin{aligned} H^2 &\ll D_2^*(H) \ll H^2, \\ H^2 \log H &\ll D_3^*(H) \ll H^2 \log H, \\ H^{n-1} &\ll D_n^*(H) \ll H^{n-1} \quad (n \geq 4). \end{aligned}$$

Comparing Theorems 1.1 with 1.4, we see that in Theorem 1.4 there is an extra factor of  $H$ . This phenomenon occurs naturally in this kind of problems: compare, for instance, [5] (monic case) with [12] and [18] (general case), or [10] (monic case) with [16] (both cases; see also [15]). In Section 5 we shall state Theorems 5.1 and 5.2 that are analogues of Theorems 1.2 and 1.3 with an extra factor of  $H$  (except for reducible quadratic polynomials when the bounds in monic and arbitrary cases are different,  $\sqrt{H}$  and  $H \log H$ , respectively).

In the next section we give some preliminaries. In Sections 3 and 4 we obtain sharp bounds for  $I_n(H)$  (proving Theorem 1.2) and for  $R_n(H)$  (proving Theorem 1.3), respectively. In Section 5 we will complete the proof of Theorem 1.4. Finally, in Section 6 we will give some explicit formulas and evaluate some constants in our formulas for polynomials of low degree.

## 2. PRELIMINARIES

In this section, we gather some preliminaries that will be useful later on.

Given a polynomial

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n = a_0 (X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{C}[X],$$

where  $a_0 \neq 0$ , its *height* is defined by  $H(f) = \max_{0 \leq j \leq n} |a_j|$ , and its *Mahler measure* by

$$M(f) = |a_0| \prod_{j=1}^n \max\{1, |\alpha_j|\}.$$

For each  $f \in \mathbb{C}[x]$  of degree  $n$ , these quantities are related by the following well-known inequality

$$H(f)2^{-n} \leq M(f) \leq H(f)\sqrt{n+1},$$

for instance, see [26, (3.12)]. So, for fixed  $n$ , we have

$$(2.1) \quad H(f) \ll M(f) \ll H(f).$$

Let  $\rho_k(n, H)$  be the number of monic polynomials

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X], \quad n \geq 2,$$

which are reducible in  $\mathbb{Z}[X]$  with an irreducible factor of degree  $k$ ,  $1 \leq k \leq n/2$ , satisfying

$$H(f) \leq H.$$

In [25], van der Waerden proved the following sharp lower and upper bounds for  $\rho_k(n, H)$ ; see also [5].

**Lemma 2.1.** *For integers  $n \geq 3$  and  $k \geq 1$ , we have*

$$\begin{aligned} H^{n-k} &\ll \rho_k(n, H) \ll H^{n-k} \quad \text{if } 1 \leq k < n/2, \\ H^{n-k} \log H &\ll \rho_k(n, H) \ll H^{n-k} \log H \quad \text{if } k = n/2. \end{aligned}$$

This yields the following corollary.

**Corollary 2.2.** *The number of reducible monic integer polynomials of degree  $n \geq 3$  and height at most  $H$  is  $O(H^{n-1})$ .*

The asymptotical formula for the number of such polynomials was given by Chela in [5].

Similarly, if  $\rho_k^*(n, H)$  is the number of polynomials

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X], \quad a_0 \neq 0, n \geq 2,$$

which are reducible in  $\mathbb{Q}[X]$  with an irreducible factor of degree  $k$ ,  $1 \leq k < n/2$ , and satisfy  $H(f) \leq H$ , then, by Theorem 4 of [18], we have the following:

**Lemma 2.3.** *For integers  $n \geq 3$  and  $k \geq 1$ , we have*

$$H^{n-k+1} \ll \rho_k^*(n, H) \ll H^{n-k+1} \quad \text{if } 1 \leq k < n/2.$$

Furthermore, the number of reducible integer polynomials of degree  $n \geq 3$  and height at most  $H$  is  $O(H^n)$ .

The asymptotical formula for the number of reducible integer polynomials of degree  $n \geq 2$  and height at most  $H$  with a quite complicated constant was recently given in [12] (see [22, Example 266], [8] and [18] for some previous bounds in this problem). Many results and asymptotic formulas counting algebraic numbers of fixed degree and bounded heights (but other than naive height) have been obtained in [6] (Mahler measure), [19], [21] (multiplicative height) and in some very recent papers [1], [2].

Some special forms of polynomials will play an important role in getting lower and upper bounds. The one below is nontrivial. It was obtained by Ferguson [14]; see also the previous result of Boyd [3].

**Lemma 2.4.** *If  $f \in \mathbb{Z}[X]$  is an irreducible polynomial which has  $m$  roots on a circle  $|z| = c$ , at least one of which is real, then one has  $f(X) = g(X^m)$ , where the polynomial  $g \in \mathbb{Z}[X]$  has at most one real root on any circle in the plane.*

The following lemma concerning the upper bound of the moduli of roots of polynomials is a classical result due to Cauchy [4] (see also [20, Theorem 2.5.1] or [23, Theorem 1.1.3]).

**Lemma 2.5.** *All the roots of the polynomial of degree  $n \geq 1$*

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{C}[X],$$

*where  $a_0 \neq 0$  and  $(a_1, \dots, a_n) \neq (0, \dots, 0)$ , are contained in the disc  $|z| \leq R$ , where  $R$  is the unique positive solution of the equation*

$$(2.2) \quad |a_0|X^n - |a_1|X^{n-1} - \cdots - |a_{n-1}|X - |a_n| = 0.$$

*In particular, when  $f \in \mathbb{R}[X]$  is the left-hand side of (2.2), then  $X = R$  is the unique positive root of  $f$ .*

This lemma will assist us in constructing irreducible degenerate polynomials explicitly.

We also need the next result about the resultant of the polynomials  $f(X)$  and  $f(\eta X)$ , where  $\eta \neq 1$ .

**Lemma 2.6.** *Let  $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n$  be a polynomial of degree  $n \geq 2$  and with unknown integer coefficients, and let  $\eta \neq 1$  be a complex number. Assume that  $f(X) \neq f(\eta X)$ . Then, for any fixed  $a_0, a_1, \dots, a_{n-1}$ , the resultant  $\text{Res}(f(X), f(\eta X))$  is a non-zero polynomial in  $a_n$  of degree at most  $n$ .*

*Proof.* Assume that  $x$  is a common root of  $f(X)$  and  $f(\eta X)$ . Then,  $x$  is also a root of  $f(X) - f(\eta X)$ . Since  $f(X) - f(\eta X)$  is a non-zero polynomial, there are at most  $n$  values of  $x$  for which  $f(x) - f(\eta x) = 0$ .

Now, let us fix  $a_0, a_1, \dots, a_{n-1}$ . Suppose that  $\text{Res}(f(X), f(\eta X))$  is zero identically. Then, for any  $a_n \in \mathbb{Z}$ ,  $f(X)$  and  $f(\eta X)$  have common roots. Since there are at most  $n$  values for those possible common roots, there exist  $a_n, a'_n \in \mathbb{Z}$ ,  $a_n \neq a'_n$ , such that the two polynomials  $a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n$  and  $a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a'_n$  have common roots. But this is possible only if  $a_n = a'_n$ , which leads to a contradiction. In addition, by the definition of the resultant by a Sylvester matrix, it is easy to see that the degree of the polynomial  $\text{Res}(f(X), f(\eta X))$  in  $a_n$  is at most  $n$ .  $\square$

This gives the next upper bounds for  $D_n(H)$  (and  $D_n^*(H)$ ), which (although they are not sharp for  $n > 2$ ) will be useful afterwards.

**Proposition 2.7.** *For each integer  $n \geq 2$ , we have  $D_n(H) = O(H^{n-1})$  and  $D_n^*(H) = O(H^n)$ .*

*Proof.* Notice that, for fixed  $n \geq 2$ , there are only finitely many roots of unity which are ratios of two algebraic numbers of degree at most  $n$ . (See, e.g., [17] or [9, Corollary 1.3] for a more precise result asserting that  $\deg(\alpha/\alpha') \leq \deg \alpha$  whenever  $\alpha, \alpha'$  are two conjugate algebraic numbers whose quotient  $\alpha/\alpha'$  is a root of unity.)

If  $f(X) = a_0X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$  is degenerate, then there exists a root of unity  $\eta \neq 1$  which is the ratio of two distinct roots of  $f$  (note that there are only finitely many values for such  $\eta$ ). So,  $f(X)$  and  $f(\eta X)$  have a common root. Hence, the resultant

$$R_\eta(a_0, a_1, \dots, a_n) = \text{Res}(f(X), f(\eta X))$$

vanishes. Furthermore, viewing  $R_\eta(a_0, a_1, \dots, a_n)$  as a polynomial with respect to  $a_0, a_1, \dots, a_n$ , every point  $(a_0, a_1, \dots, a_n)$  at which  $R_\eta$  vanishes corresponds to a degenerate polynomial  $f$ .

Clearly, the number of such polynomials  $f$  with  $a_{n-1} = 0$  is  $O(H^n)$ . Now, let us assume that  $a_{n-1} \neq 0$ . Then  $f(X) \neq f(\eta X)$ . By Lemma 2.6, if we fix  $a_0, a_1, \dots, a_{n-1}$ ,  $R_\eta(a_0, a_1, \dots, a_n)$  is a non-zero polynomial in  $a_n$  of degree at most  $n$ . Thus, there are at most  $n$  values of  $a_n$ . Hence, the equation  $R_\eta(a_0, a_1, \dots, a_n) = 0$  has  $O(H^n)$  integer solutions in variables  $a_0, a_1, \dots, a_n$  with  $|a_0|, |a_1|, \dots, |a_n| \leq H$ . Finally, by summing up the number of these integer solutions running through all possible values of  $\eta$ , we get  $D_n^*(H) = O(H^n)$ .

In the monic case, the value of  $a_0$  is fixed,  $a_0 = 1$ , so, for  $D_n(H)$ , we obtain  $D_n(H) = O(H^{n-1})$ .  $\square$

### 3. SHARP BOUNDS FOR $I_n(H)$

In this section, we will obtain sharp bounds for  $I_n(H)$  (this is perhaps the most difficult part of the paper).

Let  $f \in \mathbb{Z}[X]$  be an irreducible polynomial of degree  $n \geq 2$ . We say that two of its roots  $\alpha$  and  $\beta$  belong to the same equivalence class if their quotient is a root of unity. Suppose that there are  $s(f)$  distinct equivalence classes. Using the Galois action on the roots of  $f$ , it is easy to see that each equivalence class contains the same number of elements, say,  $\ell(f)$  roots of  $f$ . Thus, as in [11] (see also [24]), we have

$$(3.1) \quad n = s(f)\ell(f).$$

Clearly, any irreducible polynomial  $f \in \mathbb{Z}[X]$  is degenerate if and only if  $\ell(f) \geq 2$ . From now on, we will concentrate on monic polynomials and then explain in Section 5 the differences in the general (non-monic) case.

For integers  $n \geq 2, \ell \geq 2$ , we define the set

$$S_{n,\ell}(H) = \{f \in S_n(H) : f \text{ is irreducible, } \ell(f) = \ell\}.$$

Then, putting  $I_{n,\ell}(H) = |S_{n,\ell}(H)|$ , we have

$$I_n(H) = \sum_{\ell=2}^n I_{n,\ell}(H).$$

Evidently, by (3.1), we have  $I_{n,\ell}(H) = 0$  when  $\ell$  does not divide  $n$ . If  $n$  is an integer greater than 1 and  $\ell|n$ , we can get the following sharp bounds for  $I_{n,\ell}(H)$ :

**Proposition 3.1.** *For any integer  $n \geq 2$  and its any divisor  $\ell \geq 2$ , we have*

$$H^{n/\ell} \ll I_{n,\ell}(H) \ll H^{n/\ell}.$$

*Proof.* Take any polynomial  $f \in S_{n,\ell}(H)$ . Denote, for brevity,  $\ell(f) = \ell$  and  $s(f) = s$ . Suppose that the  $s$  equivalence classes of roots of  $f$  are  $C_1, \dots, C_s$ . Let  $\beta_j$  be the product of all the elements of  $C_j$ ,  $1 \leq j \leq s$ . Then, every automorphism of the Galois group of  $\text{Gal}(K/\mathbb{Q})$ , where  $K$  is the splitting field of  $f$ , which maps an element of  $C_i$  into an element of  $C_j$ , maps a root of unity into a root of unity, so it maps all  $\ell$  elements of  $C_i$  into  $\ell$  elements of  $C_j$ . Thus,  $\beta_1, \dots, \beta_s$  are conjugate algebraic numbers. Hence,

$$(3.2) \quad g(X) = (X - \beta_1) \cdots (X - \beta_s) \in \mathbb{Z}[X].$$

We claim that there are only finitely many polynomials  $f$  corresponding to the same  $g$ . Indeed, for  $1 \leq j \leq s$ , since the quotient of any two elements of  $C_j$  is a root of unity, we have  $\beta_j = \alpha_j^\ell \eta_j$  for some  $\alpha_j \in C_j$  and some root of unity  $\eta_j$ , where the degree of  $\eta_j$  is bounded above by a constant depending only on  $n$ . This implies that  $\beta_1, \dots, \beta_s$  are distinct. Now, for every fixed  $\beta_j$ , where  $1 \leq j \leq s$ , there are only



finitely many possible  $\eta_j$ , so there are also finitely many  $\alpha_j$ . Thus, if we fix  $g$  (that is, fix  $\beta_1, \dots, \beta_s$ ), then there are only finitely many of such representatives in each equivalence class  $\alpha_1 \in C_1, \dots, \alpha_s \in C_s$ . Since other roots of  $f$  have the form  $\alpha_j \xi_i$  with  $1 \leq j \leq s$  and a root of unity  $\xi_i$  of degree at most  $n$ , there are only finitely many such degenerate polynomials  $f \in \mathbb{Z}[X]$ . This completes the proof of the claim.

Note that  $M(f) = M(g)$ , so

$$H(f) \ll H(g) \ll H(f)$$

in view of (2.1). It follows that the number of such polynomials  $f \in S_{n,\ell}(H)$  is bounded above by the number of those corresponding monic polynomials  $g \in \mathbb{Z}[X]$  of degree  $s = n/\ell$  and height at most  $H$  (up to some constant), which is  $O(H^{n/\ell})$ . This proves the upper bound  $I_{n,\ell}(H) \ll H^{n/\ell}$ .

We remark that, for  $n$  odd (but only for  $n$  odd!), another proof of the inequality  $I_{n,\ell}(H) \ll H^{n/\ell}$  can be given, by applying Lemma 2.4. Indeed, take a polynomial  $f \in S_{n,\ell}(H)$ . Since  $n$  is odd,  $f$  has at least one real root. Pick one equivalence class  $C$  which has been defined above such that there is a real root  $\alpha$  of  $f$  contained in  $C$ . Notice that these  $\ell$  roots in  $C$  all have the same modulus  $|\alpha|$ . Assume that this circle contains  $t \geq 1$  equivalence classes. (In general,  $t$  can be greater than 1.) Then there are exactly  $t\ell$  conjugates of  $\alpha$  lying on the circle  $|z| = |\alpha|$  and  $\alpha$  is a real conjugate lying on  $|z| = |\alpha|$ . Hence, by Lemma 2.4, we must have  $f(X) = g(X^{t\ell})$  for some  $g \in \mathbb{Z}[X]$ . In particular, this means that the coefficient for any term  $X^k$  of the polynomial  $f$  with  $\ell \nmid k$  is zero. So, as above, we obtain  $I_{n,\ell}(H) \ll H^{n/\ell}$  (for  $n$  odd).

For the lower bound, without restriction of generality we may assume that  $H \geq 4$ . Consider monic polynomials  $g$  of degree  $m = n/\ell$  of the form

$$(3.3) \quad g(X) = X^m - 2b_1 X^{m-1} - \dots - 2b_{m-1} X - 2(2b_m - 1),$$

where  $1 \leq b_1, \dots, b_{m-1} \leq \lfloor H/2 \rfloor$  and  $1 \leq b_m \leq \lfloor H/4 \rfloor$ . There are at least  $\lfloor H/4 \rfloor^m$  of such polynomials  $g$ . They are all irreducible, by Eisenstein's criterion with respect to the prime 2. Note that if  $g$  is as above, then the polynomial  $f(X) = g(X^\ell) \in \mathbb{Z}[X]$  has degree  $n$  and height  $H(f) = H(g) \leq H$ . To complete the proof of the lower bound of the proposition, it remains to show that  $f \in S_{n,\ell}(H)$ .

By Lemma 2.5, let  $\gamma = \gamma_1$  be the unique positive root of  $g$ . By the choice of coefficients in (3.3) and in view of Lemma 2.4, the polynomial  $g$  has all its other roots  $\gamma_2, \dots, \gamma_m$  in the disc  $|z| < \gamma$ , so  $g$  is non-degenerate. Hence, none of the quotients  $\gamma_k/\gamma_j$ , where  $k \neq j$ , is a root of unity. Since the  $m\ell = n$  roots of  $f$  are exactly  $e^{2\pi i(k-1)/\ell} \gamma_j^{1/\ell}$ , where

$i = \sqrt{-1}$ ,  $1 \leq j \leq m$  and  $1 \leq k \leq \ell$ , we must have  $f \in S_{n,\ell}(H)$  if  $f$  is irreducible.

Assume that  $f$  is reducible and that its irreducible factor  $f_1 \in \mathbb{Z}[X]$  has, say,  $t \geq 1$  roots on the circle  $|z| = \gamma_1^{1/\ell}$  including the root  $\gamma_1^{1/\ell}$ . Let  $K$  be the splitting field of  $f$  over  $\mathbb{Q}$ . Since  $g$  is irreducible, for any  $2 \leq j \leq m$ , there exists an automorphism of  $\text{Gal}(K/\mathbb{Q})$  that maps  $\gamma_1$  to  $\gamma_j$ . It follows that  $\gamma_1^{1/\ell}$  has exactly  $t$  conjugates in each set  $e^{2\pi i(k-1)/\ell} \gamma_j^{1/\ell}$ , where  $i = \sqrt{-1}$ ,  $j \geq 2$  is fixed and  $k = 1, \dots, \ell$ . Thus, as  $\deg f_1 < \deg f$ , we have  $1 \leq t < \ell$  and the modulus of the product of all the conjugates of  $\gamma_1^{1/\ell}$  is equal to

$$|f_1(0)| = |\gamma_1^{t/\ell} \gamma_2^{t/\ell} \cdots \gamma_m^{t/\ell}| = |g(0)|^{t/\ell} = 2^{t/\ell} (2b_m - 1)^{t/\ell} \in \mathbb{Z}.$$

Now, it is easy to see that this is impossible, because the number  $2^{t/\ell} (2b_m - 1)^{t/\ell}$  is irrational in view of  $t < \ell$ .  $\square$

Now, we are ready to prove Theorem 1.2 which gives sharp bounds for the quantity  $I_n(H)$ .

*Proof of Theorem 1.2.* Since  $I_{n,\ell}(H) = 0$  when  $\ell$  does not divide  $n$ , we have

$$I_n(H) = \sum_{\ell=2, \ell|n}^n I_{n,\ell}(H).$$

The desired result follows immediately from Proposition 3.1, since the largest contribution comes from the term  $I_{n,p}(H)$ , where  $p$  is the smallest prime divisor of  $n$ .  $\square$

#### 4. SHARP BOUNDS FOR $R_n(H)$

In order to get an upper bound for  $R_n(H)$ , we need the following lemma, which may be of independent interest.

**Lemma 4.1.** *For each integer  $n \geq 4$ , the number of polynomials, contained in  $S_n(H)$  and having a linear factor, is bounded above by  $O(H^{n-2})$ .*

*Proof.* Every polynomial  $f$  we consider has the following form

$$f = g(X)h(X) \in S_n(H),$$

where  $g(X) = X + a$  for some  $a \in \mathbb{Z}$ , and  $h(X)$  is a monic integer polynomial of degree  $n - 1$ . Since  $M(f) = M(g)M(h)$ , we have

$$H(f) \ll H(g)H(h) \ll H(f).$$

Note that the implied constants depend only on the degree  $n$ , and are independent of  $f, g$  and  $h$ . If  $H(g) = k \leq H$  (that is,  $a = \pm k$  for

$k \geq 2$ , and  $a = 0, \pm 1$  for  $k = 1$ ), then we have  $H(h) \ll H/k$  for each  $k = 1, \dots, H$ .

Since  $f$  is degenerate,  $h$  is either degenerate or it has the linear factor  $X - a$  (and so  $a \neq 0$ , and  $h$  of degree  $n - 1$  is reducible). In both cases, either by Proposition 2.7 or by Corollary 2.2, the number of such polynomials  $h$  is  $O((H/k)^{n-2})$ . Notice that the constants implied in the symbols  $\ll$  and  $O$  depend only on  $n$  and are independent of  $k$  and  $H$ , so we can sum them up. Then, the number of such polynomials  $f$  can be bounded above by

$$(4.1) \quad \sum_{k=1}^H (H/k)^{n-2} < H^{n-2} \sum_{k=1}^{\infty} (1/k)^{n-2} = \zeta(n-2) H^{n-2}$$

up to some constant, where  $\zeta$  is the Riemann zeta function. Note that  $\zeta(m) \leq \zeta(2) = \pi^2/6$  for any integer  $m \geq 2$ . Since  $n \geq 4$ , we finally get the desired upper bound  $O(H^{n-2})$ .  $\square$

In fact, for  $n \geq 4$ , notice that any polynomial  $(X^2 - 1)g(X)$ , where  $g$  is a monic polynomial with integer coefficients of degree  $n - 2$  and height  $\leq \lfloor H/2 \rfloor$ , is contained in  $S_n(H)$  and has a linear factor. Hence, the number of reducible polynomials, contained in  $S_n(H)$  and having a linear factor, is bounded below by  $H^{n-2}$  up to some constant. Thus, combining with Lemma 4.1, we get sharp bounds for the number of such polynomials.

Below, we first deduce an upper bound for  $R_n(H)$ ,  $n \geq 5$ , and then deal with the exceptional cases  $n = 3, 4$ . These exceptional cases will be treated in a more general way that can be easily extended to count non-monic degenerate polynomials in Section 5.

**Proposition 4.2.** *For  $n \geq 5$ , we have  $R_n(H) \ll H^{n-2}$ .*

*Proof.* Since  $n \geq 5$ , by Lemma 2.1, the number of reducible polynomials  $f \in S_n(H)$  whose irreducible factor with smallest degree has degree greater than 1 is  $O(H^{n-2})$ . So, we only need to consider those reducible polynomials  $f \in S_n(H)$  which have a linear factor. Then, the desired result follows directly from Lemma 4.1.  $\square$

**Proposition 4.3.** *We have  $R_3(H) \ll H \log H$ .*

*Proof.* Note that any reducible polynomial  $f \in S_3(H)$  must have the form

$$f(X) = g(X)h(X) \in S_3(H),$$

where  $g(X) = X + a$  for some  $a \in \mathbb{Z}$ , and  $h(X)$  is a quadratic degenerate monic polynomial. (In case  $h$  is not degenerate it must be of the form  $h(X) = (X - a)(X + b)$  with  $a, b \in \mathbb{Z}$ . Then, we can simply

replace the pair  $(g(X), h(X)) = (X + a, (X - a)(X + b))$  by the pair  $(g(X), h(X)) = (X + b, (X - a)(X + a))$ . As the proof of Lemma 4.1, using Proposition 2.7, we see that the number of such polynomials  $f$  can be bounded above by

$$(4.2) \quad \sum_{k=1}^H H/k = H \sum_{k=1}^H 1/k \ll H \log H$$

up to some constant.  $\square$

**Proposition 4.4.** *We have  $R_4(H) \ll H^2$ .*

*Proof.* By Lemma 4.1, the number of polynomials contained in  $S_4(H)$  and having a linear factor is bounded above by  $O(H^2)$ . So, we only need to count those polynomials which can be factored into the product of two irreducible quadratic polynomials. Let

$$f(X) = g(X)h(X) \in S_4(H),$$

where  $g$  and  $h$  are irreducible quadratic monic polynomials.

Suppose first that both  $g$  and  $h$  are non-degenerate with roots  $\alpha, \alpha'$  and  $\beta, \beta'$ , respectively. Since  $f$  is degenerate, there exist a root, say  $\alpha$ , of  $g$  and a root, say  $\beta$ , of  $h$  such that  $\alpha/\beta = \eta$  is a root of unity. Then, mapping  $\alpha$  to  $\alpha'$  we obtain  $\alpha' = \beta'\eta'$  with a root of unity  $\eta'$ . (If  $\alpha' = \beta\eta'$ , then the quotient  $\alpha/\alpha' = \eta/\eta'$  is a root of unity, which is not the case.) From  $\alpha\alpha' = \beta\beta'\eta\eta'$  we deduce that  $\eta\eta' = \pm 1$ , since  $\alpha\alpha', \beta\beta' \in \mathbb{Z}$ . Thus,  $g(X) = X^2 + uX + v \in \mathbb{Z}[X]$  and  $h(X) = X^2 + wX \pm v \in \mathbb{Z}[X]$ . From  $v^2 \leq H$  and  $\max(|uw|, |2v + uw|) \leq H$ , we derive that  $|v| \leq \sqrt{H}$  and  $|uw| \leq H + 2\sqrt{H}$ . Hence, for  $H$  large enough, the number of such integer triplets  $(u, w, v)$  is bounded above by  $O(H^{3/2} \log H) = O(H^2)$ .

From now on, we assume that at least one of  $g$  and  $h$  is degenerate. Without loss of generality, we assume that  $g$  is degenerate. Here, we briefly follow the proof of Lemma 4.1. Notice that  $M(f) = M(g)M(h)$ . Thus,

$$H(f) \ll H(g)H(h) \ll H(f).$$

If  $H(g) = k \leq H$ , where  $k \in \mathbb{N}$ , then  $H(h) \ll H/k$ , so the number of such polynomials  $h$  is  $O((H/k)^2)$ , and, as the proof of Proposition 2.7, there are finitely many choices of  $g$  (since we choose one coefficient to be  $\pm k$ ). Then, the number of such polynomials  $f$  can be bounded above by

$$(4.3) \quad \sum_{k=1}^H (H/k)^2 < H^2 \sum_{k=1}^{\infty} 1/k^2 = \zeta(2)H^2$$

up to some constant.

Summarizing, we obtain  $R_4(H) \ll H^2$ .  $\square$

Finally, as an application of the above results, we complete the proof of Theorem 1.3.

*Proof of Theorem 1.3.* Evidently, each reducible polynomial  $f \in S_2(H)$  must have the form  $f(X) = X^2 - a^2$  for some  $a \in \mathbb{N}$  satisfying  $a^2 \leq H$ . Hence,  $R_2(H) = \lfloor \sqrt{H} \rfloor$ .

Note that Propositions 4.2, 4.3 and 4.4 give the required upper bounds, so we only need to prove the lower bounds on  $R_n(H)$  for  $n \geq 3$ .

Notice that, for any  $a, b \in \mathbb{N}$ , the polynomial

$$f(X) = (X + a)(X^2 + b) = X^3 + aX^2 + bX + ab$$

is reducible and degenerate. Since different pairs  $(a, b)$  give different polynomials, and  $f \in S_3(H)$  when  $ab \leq H$ , we find that

$$R_3(H) \geq \sum_{k=1}^H \lfloor H/k \rfloor.$$

By the properties of harmonic series, we obtain  $R_3(H) \gg H \log H$ .

Similarly, for  $n \geq 4$ , we consider

$$f(X) = (X^2 + 1)g(X) \in \mathbb{Z}[X]$$

with  $g(X) = X^{n-2} + b_1X^{n-3} + \dots + b_{n-2} \in \mathbb{Z}[X]$  whose coefficients satisfy  $1 \leq b_1, \dots, b_{n-2} \leq \lfloor H/2 \rfloor$ . Obviously, such  $f$  is reducible, degenerate and of height at most  $H$ . There are exactly  $\lfloor H/2 \rfloor^{n-2}$  of such polynomials. Consequently,  $R_n(H) \gg H^{n-2}$ .  $\square$

## 5. PROOF OF THEOREM 1.4

In order to prove Theorem 1.4, we first state the following sharp bounds for  $I_n^*(H)$  and  $R_n^*(H)$ , respectively.

**Theorem 5.1.** *Let  $n \geq 2$  and  $H \geq 1$  be two integers, and let  $p$  be the smallest prime divisor of  $n$ . Then*

$$H^{1+n/p} \ll I_n^*(H) \ll H^{1+n/p}.$$

**Theorem 5.2.** *For integers  $n \geq 2$  and  $H \geq 2$ , we have*

$$H \log H \ll R_2^*(H) \ll H \log H,$$

$$H^2 \log H \ll R_3^*(H) \ll H^2 \log H,$$

$$H^{n-1} \ll R_n^*(H) \ll H^{n-1} \quad (n \geq 4).$$

We remark that, unlike in all formulas of Theorems 5.1 and 5.2, the size of  $R_2^*(H)$  is not related to  $R_2(H) = \lfloor \sqrt{H} \rfloor$  by adding an extra power of  $H$ .

In the following, we want to briefly follow the deductions in the previous sections to prove Theorems 5.1 and 5.2. Then, Theorem 1.4 follows directly.

*Proof of Theorem 5.1.* We define  $I_{n,\ell}^*(H)$  as the number of irreducible polynomials  $f \in S_n^*(H)$  such that  $\ell(f) = \ell$ , and write  $s(f)$  as  $s$ , where  $\ell(f)$  and  $s(f)$  have been defined in (3.1). Obviously,

$$I_n^*(H) = \sum_{\ell=2, \ell|n}^n I_{n,\ell}^*(H).$$

As Section 3, following the proof of Proposition 3.1, we replace the  $g(X)$  given in (3.2) by

$$g(X) = a_0(X - \beta_1) \cdots (X - \beta_s) \in \mathbb{Z}[X],$$

where  $a_0$  is the leading coefficient of the corresponding polynomial  $f$ . Here,  $g \in \mathbb{Z}[X]$ , since any product  $a_0 \prod_{j \in I} \alpha_j$ , where  $\alpha_1, \dots, \alpha_n$  are the roots of  $f$  and  $I$  is a subset of the set  $\{1, 2, \dots, n\}$ , is an algebraic integer. Now, as in Proposition 3.1, this gives the upper bound  $I_n^*(H) \ll H^{1+n/\ell}$ .

For the lower bound, instead of (3.3), we consider

$$g(X) = (2b_0 - 1)X^m - 2b_1X^{m-1} - \cdots - 2b_{m-1}X - 2(2b_m - 1) \in \mathbb{Z}[X],$$

where  $1 \leq b_0, b_1, \dots, b_{m-1} \leq \lfloor H/2 \rfloor$ ,  $1 \leq b_m \leq \lfloor H/4 \rfloor$ . There are at least  $\lfloor H/4 \rfloor^{m+1}$  of such polynomials  $g$  for  $H \geq 4$ . As before, by Lemmas 2.4 and 2.5, let  $\gamma$  be the unique positive root of  $g$ , its other roots  $\gamma_2, \dots, \gamma_m$  lie in the disc  $|z| < \gamma$ , so  $g$  is non-degenerate. Since  $m = n/\ell$ , for  $\ell|n$  (and  $\ell \geq 2$ ), as in the proof of Proposition 3.1, we deduce that

$$H^{1+n/\ell} \ll I_{n,\ell}^*(H) \ll H^{1+n/\ell},$$

which implies Theorem 5.1.  $\square$

*Proof of Theorem 5.2.* To get an analogue of Lemma 4.1, we note that the form of  $f$  of degree  $n \geq 4$  becomes

$$f(X) = g(X)h(X) \in S_n^*(H),$$

where  $g(X) = a_0X + a_1$ , and  $h(X)$  is an integer polynomial of degree  $n-1$ . Fix an integer  $k$  with  $1 \leq k \leq H$ , let  $H(g) = k$ , then the number of such polynomials  $g$  with  $H(g) = k$  is  $O(k)$ , and as before, we have  $H(h) \ll H/k$ . Since  $f$  is degenerate,  $h$  is either degenerate or it has the linear factor  $a_0X - a_1$  (and so  $a_1 \neq 0$ , and  $h$  of degree  $n-1$  is

reducible). In both cases, either by Proposition 2.7 or, this time, by Lemma 2.3, the number of such polynomials  $h$  is  $O((H/k)^{n-1})$ . Then, the bound in (4.1) becomes

$$\sum_{k=1}^H k(H/k)^{n-1} < H^{n-1} \sum_{k=1}^{\infty} (1/k)^{n-2} = \zeta(n-2)H^{n-1},$$

which implies the desired upper bound  $O(H^{n-1})$  for  $n \geq 4$ . Then as the proof of Proposition 4.2 (this time, applying Lemma 2.3), we get the analogue of Proposition 4.2

$$R_n^*(H) \ll H^{n-1} \quad \text{for each } n \geq 5.$$

Following the proof of Proposition 4.3, we replace the form of  $f$  by  $f = g(X)h(X) \in S_3^*(H)$ , where  $g(X) = a_0X + a_1$ , and  $h(X)$  is a quadratic degenerate polynomial. Note that the number of such polynomials  $g$  with  $H(g) = k$  is  $O(k)$  for every  $k \in \mathbb{N}$ . Using Proposition 2.7, we see that the bound in (4.2) becomes

$$\sum_{k=1}^H k(H/k)^2 = H^2 \sum_{k=1}^H 1/k \ll H^2 \log H.$$

Consequently,

$$R_3^*(H) \ll H^2 \log H,$$

which is the analogue of Proposition 4.3.

To get an upper bound for  $R_4^*(H)$ , we should change the form of  $f$  in the proof of Proposition 4.4 to be

$$f(X) = g(X)h(X) \in S_4^*(H),$$

where  $g$  and  $h$  are irreducible quadratic polynomials.

Assume that both  $g$  and  $h$  are non-degenerate. We also borrow the notation from the proof of Proposition 4.4. Since  $f$  is degenerate, there exist a root  $\alpha$  of  $g$  and a root  $\beta$  of  $h$  such that  $\alpha/\beta = \eta$  is a root of unity. Multiplying with  $\alpha' = \beta'\eta'$ , we find that  $\alpha\alpha' = \beta\beta'\eta\eta'$ . Hence,  $\eta\eta' = \pm 1$ , since  $\alpha\alpha', \beta\beta' \in \mathbb{Q}$ . Thus,  $g(X) = tX^2 + uX + v \in \mathbb{Z}[X]$  and  $h(X) = t_1X^2 + wX + v_1 \in \mathbb{Z}[X]$ , where

$$(5.1) \quad |v/t| = |v_1/t_1|.$$

Without restriction of generality, we may assume that  $g$  is primitive, namely, no prime  $p$  divides all three coefficients  $t, u, v$  of  $g$ .

Suppose first that both pairs  $\alpha, \alpha'$  and  $\beta, \beta'$  are real. Then  $\eta = \alpha/\beta = -1$  and  $\eta' = \alpha'/\beta' = -1$ . So, if  $g(X) = tX^2 + uX + v \in \mathbb{Z}[X]$ , then  $h(X) = c(tX^2 - uX + v)$  with some non-zero  $c \in \mathbb{Z}$ . Since the Mahler measures of  $g$  and  $h/c$  are the same, we have  $H(g) \ll$

$M(g) \ll \sqrt{H/|c|}$ . This gives the following upper bound for the number of  $(t, u, v, c) \in \mathbb{Z}^4$

$$\sum_{|c|=1}^H |c|(H/|c|)^{3/2} = H^{3/2} \sum_{|c|=1}^H |c|^{-1/2} \ll H^2$$

up to some constant.

Suppose next that at least one pair of conjugates, say  $\beta, \beta'$ , are complex (non-real) numbers. Then they are complex conjugates. Moreover, the conjugates  $\alpha$  and  $\alpha'$  have the same moduli. Since  $\alpha/\alpha' \neq -1$ , the numbers  $\alpha, \alpha'$  are also complex conjugate numbers. From

$$|\alpha| = |\alpha'| = |\beta| = |\beta'| = R > 0$$

and

$$g(X)h(X) = (tX^2 + uX + v)(t_1X^2 + wX + v_1),$$

we find that  $|vv_1| \leq H$  and  $|tt_1| \leq H$ . Consider irreducible rational fraction  $a/b$  with  $a, b \in \mathbb{N}$  satisfying  $ab \leq H$ . Let  $(v_1, v, t_1, t) \in \mathbb{Z}^4$  be a vector satisfying  $|v_1|/|v| = |t_1|/|t| = a/b$  (see (5.1)), where  $1 \leq ab, |tt_1|, |vv_1| \leq H$ . Then, for some  $s, s_1 \in \mathbb{N}$ , we must have

$$|v_1| = sa, \quad |v| = sb, \quad |t_1| = s_1a, \quad |t| = s_1b,$$

so that  $s, s_1 \leq \sqrt{H/ab}$ . This gives at most  $ss_1 \leq H/ab$  vectors  $(|v_1|, |v|, |t_1|, |t|) \in \mathbb{N}^4$  corresponding to the fixed fraction  $a/b$ . Therefore, the number of such vectors  $(v_1, v, t_1, t) \in \mathbb{Z}^4$  is bounded from above (up to some constant) by

$$\sum_{a=1}^H \sum_{b=1}^{\lfloor H/a \rfloor} \frac{H}{ab} = O(H(\log H)^2).$$

Also,  $u = -t(\alpha + \alpha')$ , so

$$|u| \leq |t|(|\alpha| + |\alpha'|) = 2|t|R = 2|t|\sqrt{|v|/t} = 2\sqrt{|vt|}.$$

Similarly,  $|w| \leq 2\sqrt{|v_1t_1|}$ . Thus,  $|uw| \leq 4\sqrt{|vtv_1t_1|} \leq 4H$ . Clearly, there are  $O(H \log H)$  of such pairs  $(u, w) \in \mathbb{Z}^2$ . Therefore, in case  $\beta, \beta'$  are complex (non-real) numbers, we bound the number of vectors  $(v_1, v, t_1, t, u, w) \in \mathbb{Z}^6$  from above by  $O(H^2(\log H)^3)$ .

Summarizing, when none of the quadratic factors  $g$  and  $h$  is degenerate, the bound is  $O(H^2(\log H)^3)$ , which is better than the required bound  $O(H^3)$ .

It remains to consider the case when at least one of the factors  $g, h$ , say  $g$ , is degenerate. Then, in view of Proposition 2.7, the bound in



(4.3) becomes

$$\sum_{k=1}^H k(H/k)^3 < H^3 \sum_{k=1}^{\infty} 1/k^2 = \zeta(2)H^3.$$

This yields the required analogue of Proposition 4.4, namely,

$$R_4^*(H) \ll H^3.$$

Now, we will complete the proof of Theorem 5.2. It is easy to see that each reducible polynomial  $f \in S_2^*(H)$  must be of the form

$$f(X) = \pm c(a^2X^2 - b^2)$$

for some  $a, b \in \mathbb{N}$  and some square-free  $c \in \mathbb{N}$ . From  $1 \leq c \leq H$  and  $1 \leq a, b \leq \lfloor \sqrt{H/c} \rfloor$ , we obtain

$$(5.2) \quad R_2^*(H) = 2 \sum_{c=1, c \text{ square-free}}^H \lfloor \sqrt{H/c} \rfloor^2.$$

Using the fact that the sum  $\sum' 1/c$  taken over square-free  $c$  in the range  $1 \leq c \leq H$  satisfies  $\log H \ll \sum' 1/c \ll \log H$ , we obtain the required bounds  $H \log H \ll R_2^*(H) \ll H \log H$ .

To get a lower bound for  $R_3^*(H)$  observe that, for any  $a, b, c, d \in \mathbb{N}$ , the polynomial

$$f(X) = (aX + b)(cX^2 + d) = acX^3 + bcX^2 + adX + bd$$

is reducible and degenerate. Moreover, if  $c$  and  $d$  are coprime, then different integer vectors  $(a, b, c, d) \in \mathbb{Z}^4$  give different  $f$ . By counting all the vectors  $(a, b, c, d) \in \mathbb{N}^4$  satisfying  $1 \leq a \leq b \leq H, 1 \leq c, d \leq H/b$ , we find that there are exactly

$$\sum_{b=1}^H b \lfloor H/b \rfloor^2 \gg H^2 \log H$$

of them. The probability that two integers are coprime is  $1/\zeta(2)$ . So, taking into account only coprime pairs  $(c, d)$  in the above sum, we will still get  $\gg H^2 \log H$  of such vectors  $(a, b, c, d)$  (with another constant implied in  $\gg$  and not depending on  $H$ ). Consequently, we obtain  $R_3^*(H) \gg H^2 \log H$ .

Finally, for  $n \geq 4$ , let us consider

$$f(X) = (X^2 + 1)g(X) \in \mathbb{Z}[X],$$

where  $g(X) = b_0X^{n-2} + b_1X^{n-3} + \dots + b_{n-2} \in \mathbb{Z}[X]$  with coefficients  $1 \leq b_0, \dots, b_{n-2} \leq \lfloor H/2 \rfloor$ . Obviously, such  $f$  are all reducible, degenerate and have height at most  $H$ . There are exactly  $\lfloor H/2 \rfloor^{n-1}$  of such vectors

$(b_0, \dots, b_{n-2})$  and each of them gives a different polynomial  $f$ . This yields  $R_n^*(H) \gg H^{n-1}$ , and completes the proof of Theorem 5.2.  $\square$

## 6. SOME ASYMPTOTIC FORMULAS

It would be of interest to find out whether there exist asymptotic (or exact) formulas for all the quantities we consider, especially for  $D_n(H)$  and  $D_n^*(H)$ . In general, this seems to be a difficult problem, even though it is very likely that both the limits  $\lim_{H \rightarrow \infty} D_n(H)/H^{n-2}$  and  $\lim_{H \rightarrow \infty} D_n^*(H)/H^{n-1}$  exist for any  $n \geq 4$ . However, as the results of [12] indicate, one should not expect any nice formulas for the constants involved in the main terms of  $R_n(H)$  and  $R_n^*(H)$  for  $n \geq 4$ .

Here, we will consider some special cases and let the reader taste where the difficulties may come for other values of  $n$ .

**Theorem 6.1.** *For each  $H \geq 1$  we have  $R_2(H) = \lfloor \sqrt{H} \rfloor$ ,*

$$I_2(H) = 2H + \lfloor \sqrt{H} \rfloor + 2\lfloor \sqrt{H/2} \rfloor + 2\lfloor \sqrt{H/3} \rfloor,$$

$$D_2(H) = 2H + 2\lfloor \sqrt{H} \rfloor + 2\lfloor \sqrt{H/2} \rfloor + 2\lfloor \sqrt{H/3} \rfloor.$$

*Proof.* By Theorem 1.3 and  $D_2(H) = I_2(H) + R_2(H)$ , we see that it suffices to prove the formula for  $I_2(H)$ .

For any irreducible polynomial  $f \in S_2(H)$ , let  $\alpha \neq \beta$  be its roots. Then, the degree of the root of unity  $\alpha/\beta$  must be at most 2, so  $\alpha/\beta = -1, \pm i, (-1 \pm i\sqrt{3})/2$  or  $(1 \pm i\sqrt{3})/2$ , where  $i = \sqrt{-1}$ .

If  $\alpha/\beta = -1$ , we must have  $f(X) = X^2 - a$ , where  $a$  is not a perfect square and  $1 \leq |a| \leq H$ . So, the number of such polynomials  $f$  is  $2H - \lfloor \sqrt{H} \rfloor$ .

If  $\alpha/\beta = \pm i$ , we have  $f(X) = X^2 + 2aX + 2a^2$ , where  $a \in \mathbb{Z}$  and  $1 \leq |a| \leq \lfloor \sqrt{H/2} \rfloor$ . Note that each  $a$  corresponds to a different  $f$ . Clearly, the number of these polynomials  $f$  is  $2\lfloor \sqrt{H/2} \rfloor$ .

If  $\alpha/\beta = (-1 \pm i\sqrt{3})/2$ , we have  $f(X) = X^2 + aX + a^2$ , where  $a \in \mathbb{Z}$ ,  $1 \leq |a| \leq \lfloor \sqrt{H} \rfloor$ . The number of these polynomials  $f$  is  $2\lfloor \sqrt{H} \rfloor$ .

Finally, if  $\alpha/\beta = (1 \pm i\sqrt{3})/2$ , we have  $f(X) = X^2 + 3aX + 3a^2$ , where  $a \in \mathbb{Z}$  and  $1 \leq |a| \leq \lfloor \sqrt{H/3} \rfloor$ . The number of such polynomials  $f$  is  $2\lfloor \sqrt{H/3} \rfloor$ .

Summarizing the above results, we obtain exactly  $2H + \lfloor \sqrt{H} \rfloor + 2\lfloor \sqrt{H/2} \rfloor + 2\lfloor \sqrt{H/3} \rfloor$  irreducible polynomials contained in  $S_2(H)$ .  $\square$

**Theorem 6.2.** *We have  $\lim_{H \rightarrow \infty} D_3(H)/(H \log H) = 4$ .*

*Proof.* By Theorems 1.2 and 1.3, it is equivalent to prove that

$$\lim_{H \rightarrow \infty} R_3(H)/(H \log H) = 4.$$

As the proof of Proposition 4.3, any reducible polynomial  $f \in S_3(H)$  must have the form

$$f(X) = g(X)h(X) \in S_3(H),$$

where  $g(X) = X + a$  for some  $a \in \mathbb{Z}$ , and  $h(X)$  is a quadratic degenerate monic polynomial.

Let  $\alpha, \beta$  be the two distinct roots of  $h$ . Then, as above,  $\alpha/\beta = -1, \pm i, (-1 \pm i\sqrt{3})/2$  or  $(1 \pm i\sqrt{3})/2$ . If  $\alpha/\beta = -1$ , we have  $f(X) = (X + a)(X^2 + b)$ , where  $1 \leq |b| \leq H$ . Note that each pair  $(a, b)$  corresponds to a different  $f$ . So, the number of these polynomials  $f$  is exactly

$$(6.1) \quad 2 \sum_{|b|=1}^H (2\lfloor H/|b| \rfloor + 1).$$

If  $\alpha/\beta$  takes other values, then  $h$  is irreducible. Using the forms of polynomials just considered in the proof of Theorem 6.1, we can see that the number of such polynomials  $f$  is bounded above by the number of integer pairs  $(a, b)$  with  $ab^2 \leq H$  (up to some constant), which gives the term  $O(H)$ . Hence, as the main term in (6.1) is  $4H \log H$ , we obtain  $\lim_{H \rightarrow \infty} R_3(H)/(H \log H) = 4$ .  $\square$

**Theorem 6.3.** *We have*

$$\lim_{H \rightarrow \infty} I_2^*(H)/H^2 = 4,$$

$$\lim_{H \rightarrow \infty} R_2^*(H)/(H \log H) = 2/\zeta(2) = 12/\pi^2.$$

*In particular, we have  $\lim_{H \rightarrow \infty} D_2^*(H)/H^2 = 4$ .*

*Proof.* Let  $f \in S_2^*(H)$  be an irreducible polynomial, and let  $\alpha, \beta$  be its two distinct roots. Then, as before,  $\alpha/\beta = -1, \pm i, (-1 \pm i\sqrt{3})/2$  or  $(1 \pm i\sqrt{3})/2$ . Applying the same argument as the proof of Theorem 6.1, we can see that the main contribution to  $I_2^*(H)$  comes from those irreducible polynomials  $f$  with  $\alpha/\beta = -1$ , that is,  $f = aX^2 + b$ , where  $1 \leq |a|, |b| \leq H$ ,  $(a, -b) \neq \pm c(a', b')$ ,  $c \in \mathbb{N}$  is square-free, and  $a', b'$  are perfect squares. Thus,

$$\lim_{H \rightarrow \infty} I_2^*(H)/H^2 = 4.$$

Recall that, by (5.2),

$$R_2^*(H) = 2 \sum_{k=1, k \text{ is square-free}}^H \lfloor \sqrt{H/k} \rfloor^2.$$

Since every positive integer can be uniquely expressed as the product of a perfect square and a square-free integer, we have

$$\lim_{H \rightarrow \infty} \frac{\sum_{k=1, k \text{ is square-free}}^H 1/k}{\sum_{k=1}^H 1/k} = \frac{1}{\sum_{j=1}^{\infty} 1/j^2} = \frac{1}{\zeta(2)}.$$

Then, we obtain  $\lim_{H \rightarrow \infty} R_2^*(H)/(H \log H) = 2/\zeta(2)$ . The last statement of the theorem follows from  $D_2^*(H) = I_2^*(H) + R_2^*(H)$ .  $\square$

**Theorem 6.4.** *We have  $\lim_{H \rightarrow \infty} D_3^*(H)/(H^2 \log H) = 96/\pi^2$ .*

*Proof.* By Theorems 5.1 and 5.2, it is equivalent to prove that

$$\lim_{H \rightarrow \infty} R_3^*(H)/(H^2 \log H) = 96/\pi^2.$$

Recall that, any reducible polynomial  $f \in S_3^*(H)$  must have the form

$$f(X) = g(X)h(X) \in S_3^*(H),$$

where  $g(X) = aX + b$  for some  $a, b \in \mathbb{Z}$ , and  $h(X)$  is a quadratic degenerate polynomial.

As before, the main contribution to  $R_3^*(H)$  comes from those polynomials  $f$  such that the quotient of the two roots of  $h$  is  $-1$ , that is,  $f(X) = (aX + b)(cX^2 + d)$  with  $c > 0$  and  $d \neq 0$ . Without loss of generality, we may assume that  $(c, d) = 1$ , by putting their common factor into the linear factor  $aX + b$ . Note that the number of these polynomials  $f$  with  $b = 0$  is  $O(H^2)$ , so in the sequel we assume that  $b \neq 0$ .

Now, as  $1 \leq |a|, |b| \leq \min(H/c, H/|d|)$  we consider two cases  $1 \leq c < |d|$  and  $c > |d| \geq 1$  (there are two other cases with  $c = |d| = 1$ , but they only give  $O(H^2)$  of such polynomials). In the first case,  $\min(H/c, H/|d|) = H/|d|$ , the number of vectors  $(a, b, c, d)$  is

$$\begin{aligned} 8 \sum_{|d|=2}^H \lfloor H/|d| \rfloor^2 \sum_{c=1, (c, |d|)=1}^{|d|-1} 1 &\sim 8H^2 \sum_{|d|=2}^H \varphi(|d|)/|d|^2 \\ &= -8H^2 + 8H^2 \sum_{|d|=1}^H \varphi(|d|)/|d|^2 \\ &\sim (48/\pi^2)H^2 \log H, \end{aligned}$$

where  $\varphi$  is Euler's totient function,  $\sim$  is the standard asymptotic notation. (Here, we use the standard formula  $\sum_{j=1}^H \varphi(j)/j^2 \sim (6/\pi^2) \log H$ , whereas the factor 8 comes, since we have three moduli  $|a|, |b|, |d|$ .)

By exactly the same argument, we can see that the same contribution  $(48/\pi^2)H^2 \log H$  comes from the case  $c > |d| \geq 1$ . Therefore,  $\lim_{H \rightarrow \infty} R_3^*(H)/(H^2 \log H) = 96/\pi^2$ , as claimed.  $\square$

## ACKNOWLEDGEMENTS

The authors would like to thank Igor E. Shparlinski for introducing them into this topic and for providing Proposition 2.7 which was their starting point, and also for his valuable comments on an early version of this paper. The research of A. D. was supported by the Research Council of Lithuania Grant MIP-068/2013/LSS-110000-740. The research of M. S. was supported by the Australian Research Council Grant DP130100237.

## REFERENCES

- [1] F. Barroero, *Counting algebraic integers of fixed degree and bounded height*, Monatsh. Math. (to appear).
- [2] F. Barroero and M. Widmer, *Counting lattice points and o-minimal structures*, Int. Math. Res. Notices (to appear).
- [3] D. W. Boyd, *Irreducible polynomials with many roots of maximal modulus*, Acta Arith. **68** (1994), 85–88.
- [4] A. L. Cauchy, *Exercices de mathématique*, 4ème année, De Bure Frères, Paris, 1829.
- [5] R. Chela, *Reducible polynomials*, J. Lond. Math. Soc. **38** (1963), 183–188.
- [6] S. Chern and J. D. Vaaler, *The distribution of values of Mahler’s measure*, J. Reine Angew. Math. **540** (2001), 1–47.
- [7] M. Cipu, I. Diouf and M. Mignotte, *Testing degenerate polynomials*, Appl. Alg. Eng. Comm. Comp. **22** (2011), 289–300.
- [8] K. Dörge, *Abschätzung der Anzahl der reduziblen Polynome*, Math. Ann. **160** (1965), 59–63.
- [9] P. Drungilas and A. Dubickas, *On subfields of a field generated by two conjugate algebraic numbers*, Proc. Edinb. Math. Soc. **47** (2004), 119–123.
- [10] A. Dubickas, *Polynomials irreducible by Eisenstein’s criterion*, Appl. Alg. Eng. Comm. Comp. **14** (2003), 127–132.
- [11] A. Dubickas, *Roots of unity as quotients of two roots of a polynomial*, J. Aust. Math. Soc. **92** (2012), 137–144.
- [12] A. Dubickas, *On the number of reducible polynomials of bounded naive height*, Manuscr. Math. (to appear).
- [13] G. Everest, A. van der Poorten, I. E. Shparlinski and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs **104**, Amer. Math. Soc., Providence, RI, 2003.
- [14] R. Ferguson, *Irreducible polynomials with many roots of equal modulus*, Acta Arith. **78** (1997), 221–225.
- [15] R. Heyman, *On the number of polynomials of bounded height that satisfy the Dumas criterion*, J. Int. Seq. **17** (2014), Article 14.2.4, 7 p. (electronic).
- [16] R. Heyman and I. E. Shparlinski, *On the number of Eisenstein polynomials of bounded height*, Appl. Alg. Eng. Comm. Comp. **24** (2013), 149–156.
- [17] I. M. Isaacs, *Quotients which are roots of unity (solution of problem 6523)*, Am. Math. Mon. **95** (1988), 561–62.
- [18] G. Kuba, *On the distribution of reducible polynomials*, Math. Slovaca **59** (2009), 349–356.

- [19] D. Masser and J. D. Vaaler, *Counting algebraic numbers with large height*, Trans. Am. Math. Soc. II **359** (2007), 427–445.
- [20] M. Mignotte and D. Ștefănescu, *Polynomials: an algorithmic approach*, Springer, Singapore, 1999.
- [21] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.
- [22] G. Pólya and G. Szegő, *Problems and theorems in analysis, vol. II*, Springer, Berlin, Heidelberg, New York, 1976.
- [23] V. V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics **11**, Springer, Berlin, 2010.
- [24] A. Schinzel, *Around Pólya’s theorem on the set of prime divisors of a linear recurrence*, in: Diophantine equations (Saradha, N., ed.), Mumbai, India, December 16–20, 2005, New Delhi: Narosa Publishing House/Published for the Tata Institute of Fundamental Research, Studies in Mathematics, Tata Institute of Fundamental Research **20** (2008), 225–233.
- [25] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatshefte für Mathematik und Physik **43** (1936), 133–147.
- [26] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables*, Grundlehren der Mathematischen Wissenschaften **326**, Springer, Berlin, 2000.

DEPARTMENT OF MATHEMATICS AND INFORMATICS, VILNIUS UNIVERSITY,  
 NAUGARDUKO 24, LT-03225 VILNIUS, LITHUANIA  
*E-mail address:* arturas.dubickas@mif.vu.lt

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH  
 WALES, SYDNEY NSW 2052, AUSTRALIA  
*E-mail address:* shamin2010@gmail.com